PCT/JP2004/003520

日本国特許庁
JAPAN PATENT OFFICE

23.04.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

REC'D 24 JUN 2004
WIPO PCT

出願年月日
Date of Application: ２００３年　３月１７日

出願番号
Application Number: 特願２００３－０７２３７１

[ST. 10/C]: ［ＪＰ２００３－０７２３７１］

出願人
Applicant(s): セイコーエプソン株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年　６月　２日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０４７１２７

【書類名】　特許願
【整理番号】　J0096563
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/30
【発明者】
　【住所又は居所】　長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内
　【氏名】　黒田　直人
【特許出願人】
　【識別番号】　000002369
　【氏名又は名称】　セイコーエプソン株式会社
【代理人】
　【識別番号】　100095728
　【弁理士】
　【氏名又は名称】　上柳　雅誉
　【連絡先】　０２６６－５２－３１３９
【選任した代理人】
　【識別番号】　100107076
　【弁理士】
　【氏名又は名称】　藤綱　英吉
【選任した代理人】
　【識別番号】　100107261
　【弁理士】
　【氏名又は名称】　須澤　修
【手数料の表示】
　【予納台帳番号】　013044
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0109826

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ウィルス対策システムとウィルス対策プログラムとウィルス対策方法とウィルス対策用端末装置

【特許請求の範囲】

【請求項１】　周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設けた記憶手段と、

そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する手段と、

当該コンピュータの管理者宛の検出報告を発する手段と、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える手段を備えたことを特徴とするウィルス対策システム。

【請求項２】　周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶させた記憶手段と、

そのおとりアプリケーションにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する手段と、

当該コンピュータの管理者宛の検出報告を発する手段と、

当該ウィルスの駆除が完了するまで、当該コンピュータに高負荷を与える手段を備えたことを特徴とするウィルス対策システム。

【請求項３】　請求項１に記載のウィルス対策システムにおいて、

おとりフォルダは、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションから成ることを特徴とするウィルス対策システム。

【請求項４】　請求項２に記載のウィルス対策システムにおいて、

おとりアプリケーションは、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションから成ることを特徴とするウィルス対策システム。

【請求項５】　請求項１に記載のウィルス対策システムにおいて、

探索の対象となるウィルスは、共有フォルダへ侵入する性質を持つウィルスであることを特徴とするウィルス対策システム。

【請求項６】　請求項２に記載のウィルス対策システムにおいて、
探索の対象となるウィルスは、アプリケーションの誤動作を引き起こす性質を持つウィルスであることを特徴とするウィルス対策システム。
【請求項７】　請求項１または２に記載のウィルス対策システムにおいて、
感染したコンピュータに対して、高負荷を与える攻撃開始を予告するための、メッセージを送信する手段を備えたことを特徴とするウィルス対策システム。
【請求項８】　請求項１に記載のウィルス対策システムにおいて、
攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段を設けたことを特徴とするウィルス対策システム。
【請求項９】　請求項１に記載のウィルス対策システムにおいて、
コンピュータに高負荷を与える手段は、当該コンピュータのネットワークインタフェースのトラフィックを増大させる機能を持つことを特徴とするウィルス対策システム。
【請求項１０】　請求項１に記載のウィルス対策システムにおいて、
コンピュータに高負荷を与える手段は、当該コンピュータのＣＰＵが応答動作をすべき処理を大量に要求することを特徴とするウィルス対策システム。
【請求項１１】　請求項１に記載のウィルス対策システムにおいて、
ネットワークに接続された別のコンピュータに対して、ウィルスの送信元となったコンピュータのネットワークアドレスを通知するとともに、ウィルスの送信元となったコンピュータに負荷を与える処理を依頼する手段を備えたことを特徴とするウィルス対策システム。
【請求項１２】　ウィルスの送信元となったコンピュータネットワークアドレスの通知を受けたとき、ウィルスの送信元となったコンピュータに負荷を与える処理を、コンピュータに実行させるウィルス対策プログラム。
【請求項１３】　ウィルスの送信元となったコンピュータネットワークアドレスの通知を受けたとき、ウィルスの送信元となったコンピュータからの通信を拒絶する処理を、コンピュータに実行させるウィルス対策プログラム。
【請求項１４】　周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設け、

そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出し、

当該コンピュータの管理者宛の検出報告を発するとともに、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えることを特徴とするウィルス対策方法。

【請求項１５】　周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶装置に記憶させ、

そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出し、

当該コンピュータの管理者宛の検出報告を発するとともに、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えることを特徴とするウィルス対策方法。

【請求項１６】　周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを記憶させた記憶装置と、

そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出するコンピュータプログラムと、

当該コンピュータの管理者宛の検出報告を発するコンピュータプログラムと、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えるコンピュータプログラムをインストールしたことを特徴とするウィルス対策用端末装置。

【請求項１７】　周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶させた記憶装置と、

そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出するコンピュータプログラムと、

当該コンピュータの管理者宛の検出報告を発するコンピュータプログラムと、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えるコンピュータプログラムとをインストールしたことを特徴とするウィルス対策用端末装置。

【請求項１８】　周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを記憶装置に記憶させる処理と、

そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する処理と、

当該コンピュータの管理者宛の検出報告を発する処理と、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える処理とを、コンピュータに実行させることを特徴とするウィルス対策プログラム。

【請求項１９】　周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶装置に記憶させる処理と、

そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する処理と、

当該コンピュータの管理者宛の検出報告を発する処理と、

当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える処理とを、コンピュータに実行させることを特徴とするウィルス対策プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークに接続されたコンピュータがウィルスに感染したとき、感染源を突き止めて、同じネットワークに接続された他のコンピュータへの感染を阻止する機能を持つ、ウィルス対策システムとウィルス対策プログラムとウィルス対策方法とウィルス対策用端末装置に関する。

【０００２】

【従来の技術】

コンピュータウィルスには、サーバ等のコンピュータの共有フォルダに侵入して、所定のファイルやプログラムにアクセスをし、それを破壊したり、誤動作させるように書き換えたりするものがある。ウィルスの存在は、所定のプログラムを使って検出することができる。このプログラムは、ウィルスのファイル名やウィルスの行動パタンから、ウィルスであると判断をする。ウィルスを検出すると、コンピュータの管理者は必要な処置を施し、ウィルスを除去する。こうしてウ

ィルスを検出してワクチンを配布する技術は、各種紹介されている（特許文献１参照）。

【特許文献１】　特開２００２－２５９１４９号公報

【０００３】

【発明が解決しようとする課題】

ところで、上記のような従来の技術には、次のような解決すべき課題があった。

ウィルスを検出したときは、すみやかにその存在場所を突き止めて、ネットワークから切り離したり、ワクチンを用いて駆除するという処理をしなければならない。しかしながら、ウィルスを検出してから対策処理を完了するまでの間に時間がかかると、次々と被害が拡大して、ネットワークに重大な被害を及ぼす恐れもある。

また、ネットワーク上の別のコンピュータに潜んで、ネットワークを通じてファイルアクセスをしてくるようなウィルスは、活動を開始するまで検出が困難なことがある。そのウィルスが活動を開始し、ウィルスを検出したとしても、ウィルスの潜んでいるコンピュータを調べて、そのウィルスを駆除するまで時間がかかると、被害が拡大するという問題があった。

【０００４】

本発明は、以上の点に着目してなされたもので、ネットワークに接続されたコンピュータがウィルスに感染していることを突き止めると同時に、同じネットワークに接続された他のコンピュータへの被害の拡大を阻止するように、ウィルスに感染したコンピュータを攻撃する、ウィルス対策システムとウィルス対策プログラムとウィルス対策方法とウィルス対策用端末装置を提供することを目的とする。

さらに本発明は、活動を開始するまで検出活動ができないようなウィルスをいちはやく検出して、被害の拡大を抑えることができるウィルス対策システムとウィルス対策プログラムとウィルス対策方法とウィルス対策用端末装置を提供することを目的とする。

【０００５】

【課題を解決するための手段】

本発明は次の構成により上記の課題を解決する。

〈構成１〉

周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設けた記憶手段と、そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する手段と、当該コンピュータの管理者宛の検出報告を発する手段と、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える手段を備えたことを特徴とするウィルス対策システム。

【０００６】

ネットワーク監視用のコンピュータに、周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設けることで、最先にウィルスの侵入を促す。ウィルスが侵入をしたとき、直ちに感染源を突き止めて、被害の拡大を防止した上で対策を施す。ウィルスの侵入とは、ウィルスが、ネットワークを通じて、フォルダ中の任意のファイルを読み出したり、ファイルの書き換えを試みたりすることである。ウィルスに感染するというのは、ウィルス自体がコンピュータの記憶装置のどこかに取り込まれていることをいう。通信情報は、ウィルスがおとりフォルダに侵入をしたときにネットワークから受信した通信経路等の情報である。この通信情報中に、ウィルスの送信元となったコンピュータのネットワークアドレス等が含まれる。ウィルスの送信元となったコンピュータは、ウィルスに感染したコンピュータである。おとりフォルダで待ち受けるので、侵入してきたウィルスを検出できる。検出報告の内容は任意である。報告方法も任意である。感染したコンピュータの管理者に通知すると同時にその感染源のコンピュータを攻撃する。ウィルスの駆除が完了するまで、攻撃を継続する。攻撃するには、コンピュータに高負荷を与える。ウィルス対策とは、感染コンピュータをネットワークから切り離したり、あるいは、ウィルスを駆除することである。

【０００７】

〈構成２〉

周辺に設けられているアプリケーションと比較して、セキュリティの低いおと

りのアプリケーションを記憶させた記憶手段と、そのおとりアプリケーションにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する手段と、当該コンピュータの管理者宛の検出報告を発する手段と、当該ウィルスの駆除が完了するまで、当該コンピュータに高負荷を与える手段を備えたことを特徴とするウィルス対策システム。

【０００８】

構成１はおとりフォルダを設けたものであるが、構成２では、おとりアプリケーションを設ける。おとりアプリケーションにウィルスが侵入したというのは、おとりアプリケーションをアクセスしたり、おとりアプリケーションに対するコマンドを送り込んだり、おとりアプリケーションの書き換えを試みたりすることである。

【０００９】

〈構成３〉

構成１に記載のウィルス対策システムにおいて、おとりフォルダは、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションから成ることを特徴とするウィルス対策システム。

【００１０】

サーバへ侵入する性質を持つウィルスを検出する。おとりサーバは、擬似的なアプリケーションから成り、みかけ上サーバの構成を持つデータから成る。アクセスがあると、そのアクセスに対してサーバと同様の応答を返す機能を持つ。ウェブサーバでもメールサーバでも構わない。サーバ攻撃型のウィルスに対応するための構成である。コンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に、おとりフォルダを設けた構成にしたので、ウィルスの攻撃を受けてもその影響を受けない。すなわち、被害は発生しない。同時に、攻撃を受けながら、その出所を突き止めることができる。おとりサーバとおとりフォルダとは、全く別のものでも、一体化したアプリケーションから成るものでも構わない。

【００１１】

〈構成４〉

構成２に記載のウィルス対策システムにおいて、おとりアプリケーションは、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションから成ることを特徴とするウィルス対策システム。

【００１２】

これも、サーバへ侵入する性質を持つウィルス検出のための構成で、おとりフォルダの代わりにおとりアプリケーションを設けた例である。

【００１３】

〈構成５〉

構成１に記載のウィルス対策システムにおいて、探索の対象となるウィルスは、共有フォルダへ侵入する性質を持つウィルスであることを特徴とするウィルス対策システム。

【００１４】

共有フォルダへ侵入するウィルスは、おとりフォルダを設けることで、その活動を検出できる。

【００１５】

〈構成６〉

構成２に記載のウィルス対策システムにおいて、探索の対象となるウィルスは、アプリケーションの誤動作を引き起こす性質を持つウィルスであることを特徴とするウィルス対策システム。

【００１６】

アプリケーションの誤動作を引き起こす性質を持つウィルスに対しては、擬似的なおとりアプリケーションを設けることで、その活動を検出できる。

【００１７】

〈構成７〉

構成１または２に記載のウィルス対策システムにおいて、感染したコンピュータに対して、高負荷を与える攻撃開始を予告するための、メッセージを送信する手段を備えたことを特徴とするウィルス対策システム。

【００１８】

コンピュータのウィルス感染の報告をするとともに、その感染コンピュータに対して、攻撃開始を予告するメッセージを送信して、コンピュータの使用者や管理者に注意を促すことができる。

【００１９】

〈構成８〉

構成１に記載のウィルス対策システムにおいて、攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段を設けたことを特徴とするウィルス対策システム。

【００２０】

攻撃元コンピュータから警報音を発生させることで、感染コンピュータとネットワークを共有している他の端末装置の使用者に注意を促すことができる。警報音の種類は任意である。また、ディスプレイに攻撃動作中の表示をしてもよい。

【００２１】

〈構成９〉

構成１に記載のウィルス対策システムにおいて、コンピュータに高負荷を与える手段は、当該コンピュータのネットワークインタフェースのトラフィックを増大させる機能を持つことを特徴とするウィルス対策システム。

【００２２】

感染したコンピュータのネットワークインタフェースのトラフィックを増大させれば、そのネットワークインタフェースを通じた当該ウィルスによる感染の拡大が阻止できる。トラフィックを増大させる方法は任意である。

【００２３】

〈構成１０〉

構成１に記載のウィルス対策システムにおいて、コンピュータに高負荷を与える手段は、当該コンピュータのＣＰＵが応答動作をすべき処理を大量に要求することを特徴とするウィルス対策システム。

【００２４】

例えば、Ｐｉｎｇパケットを大量に連続的に送信する。これにより、ＣＰＵが過負荷になるので、コンピュータの内部でのウィルスの活動を阻止し、被害の拡

大を抑制できる。

【００２５】

〈構成１１〉

構成１に記載のウィルス対策システムにおいて、ネットワークに接続された別のコンピュータに対して、ウィルスの送信元となったコンピュータのネットワークアドレスを通知するとともに、ウィルスの送信元となったコンピュータに負荷を与える処理を依頼する手段を備えたことを特徴とするウィルス対策システム。

【００２６】

感染コンピュータへの攻撃が不十分である場合には、他のコンピュータに通知を行い、共同で攻撃をするように依頼する。依頼方法は任意である。他のコンピュータからの攻撃方法は任意である。それぞれ別々の方法でも構わない。

【００２７】

〈構成１２〉

ウィルスの送信元となったコンピュータネットワークアドレスの通知を受けたとき、ウィルスの送信元となったコンピュータに負荷を与える処理を、コンピュータに実行させるウィルス対策プログラム。

【００２８】

ネットワーク監視用のコンピュータから、感染コンピュータを攻撃する依頼を受けたときに、その処理を実行するプログラムの発明である。ネットワークに接続された任意のコンピュータにインストールされる。このコンピュータは、ネットワーク監視機能をもっていてもよいし、攻撃機能のみを持つものでもよい。

【００２９】

〈構成１３〉

ウィルスの送信元となったコンピュータネットワークアドレスの通知を受けたとき、ウィルスの送信元となったコンピュータからの通信を拒絶する処理を、コンピュータに実行させるウィルス対策プログラム。

【００３０】

ネットワーク監視用のコンピュータから、感染コンピュータの通知を受けたとき、防御のためにウィルスの送信元となったコンピュータからの通信を拒絶する

処理を実行するコンピュータプログラムの発明である。

【００３１】

〈構成１４〉

周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを設け、そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出し、当該コンピュータの管理者宛の検出報告を発するとともに、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えることを特徴とするウィルス対策方法。

【００３２】

構成１のシステムを運用する方法の発明である。

【００３３】

〈構成１５〉

周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶装置に記憶させ、そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出し、当該コンピュータの管理者宛の検出報告を発するとともに、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えることを特徴とするウィルス対策方法。

【００３４】

構成２のシステムを運用する方法の発明である。

【００３５】

〈構成１６〉

周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを記憶させた記憶装置と、そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出するコンピュータプログラムと、当該コンピュータの管理者宛の検出報告を発するコンピュータプログラムと、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えるコンピュータプログラムをインストールしたことを特徴とするウィルス対策用端末装置。

【００３６】

構成１のシステムでおとりフォルダを有する監視コンピュータの発明である。

【００３７】

〈構成１７〉

周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶させた記憶装置と、そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出するコンピュータプログラムと、当該コンピュータの管理者宛の検出報告を発するコンピュータプログラムと、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与えるコンピュータプログラムとをインストールしたことを特徴とするウィルス対策用端末装置。

【００３８】

構成２のシステムでおとりアプリケーションを有する監視コンピュータの発明である。

【００３９】

〈構成１８〉

周辺に設けられているフォルダと比較して、セキュリティの低いおとりフォルダを記憶装置に記憶させる処理と、そのフォルダにウィルスが侵入したときに取得した通信情報から、ウィルスの送信元となったコンピュータを検出する処理と、当該コンピュータの管理者宛の検出報告を発する処理と、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える処理とを、コンピュータに実行させることを特徴とするウィルス対策プログラム。

【００４０】

構成１のシステムを実現するためのコンピュータプログラムの発明である。

【００４１】

〈構成１９〉

周辺に設けられているアプリケーションと比較して、セキュリティの低いおとりのアプリケーションを記憶装置に記憶させる処理と、そのアプリケーションにウィルスがアクセスしたときに取得した通信情報から、ウィルスの送信元となっ

たコンピュータを検出する処理と、当該コンピュータの管理者宛の検出報告を発する処理と、当該ウィルスへの対策が完了するまで、当該コンピュータに高負荷を与える処理とを、コンピュータに実行させることを特徴とするウィルス対策プログラム。

【００４２】

構成２のシステムを実現するためのコンピュータプログラムの発明である。

【００４３】

【発明の実施の形態】

以下、本発明の実施の形態を、具体例を用いて説明する。

図１は、ウィルス対策システムの具体例を示すブロック図である。

ネットワーク１には、ネットワークインタフェース４を介してコンピュータ５が接続されている。このコンピュータ５には、記憶装置６が設けられている。この記憶装置６に、ウィルス７が感染している。このコンピュータ５を感染コンピュータと呼ぶことにする。ネットワーク１には、監視コンピュータ１０が接続されている。監視コンピュータ１０は、ネットワークインタフェース１１と記憶装置１２とを備える。記憶装置１２には、おとりサーバ１３と、おとりフォルダ１４と、おとりアプリケーション１５とが記憶されている。さらに、ネットワークインタフェース１１で取得される通信情報を監視するために、通信情報解析手段１６が設けられている。通信情報解析手段１６の出力は、警報発生手段１９を駆動する。さらに、通信情報解析手段１６の出力に基づいて、コンピュータ攻撃手段１７と検出報告送信手段１８とが動作するように構成されている。通信情報解析手段１６とコンピュータ攻撃手段１７と検出報告送信手段１８と警報発生手段１９はいずれも、監視コンピュータ１０に所定の処理を実行させるコンピュータプログラムである。

【００４４】

この発明は、ウィルス７に感染しているコンピュータ５を特定し、そのコンピュータ５の管理者がウィルス７を除去するまでの間、そのコンピュータ５に高負荷を生じさせ、ウィルス７の活動を抑制する。ウィルス７に感染しているコンピュータ５を特定するために、おとりサーバ１３やおとりフォルダ１４やおとりア

プリケーション１５をネットワーク１中に構築する。おとりサーバ１３等は、監視コンピュータ１０中に擬似的に生成する。おとりフォルダ１４は監視コンピュータ１０の記憶装置１２中の、任意の場所に生成するとよい。また、あるいは、おとりサーバ１３中に一体に生成する。

【００４５】

［おとりサーバ等］

おとりのサーバ１３は、ネットワーク１上で最先にウィルス７が攻撃してくるような環境設定をすることが好ましい。セキュリティを最も低くするとともに、例えば、コンピュータ名は、ネットワークコンピュータリストの最も上位に表示されるような名称に選定する。また、ウィルスを受け入れるための共有フォルダ名は、ウィルスがアタックしやすい性質のフォルダ名とする。これも、共有フォルダリストの最も上位に表示されるような名称に選定するとよい。また、コンピュータ名もフォルダ名も、ウィルスの性質から最適なものを決定するとよい。例えば、おとりサーバ１３は、ウィルス７が実在のサーバに対して侵入を試みた場合の応答と全く同様の応答をするように動作するアプリケーションプログラムからなる。実在のサーバとは異なるから、破壊活動に対しては何の影響もない。例えばフォルダ１４は、ウィルス７が実在のフォルダに対してアクセスした場合の応答と全く同様の応答をするように動作するアプリケーションプログラムからなる。実在のフォルダとは異なるからファイルの削除といった破壊活動に対して何の影響もない。おとりアプリケーション１５は、実際のアプリケーションとは異なるから、誤動作を引き起こされる恐れはない。

【００４６】

［感染コンピュータの特定］

通信情報解析手段１６には、ウィルスの侵入を検出すると、直ちにその通信情報中から発信源のコンピュータ名を解析して、特定する機能を持つ。この情報には、誰がログオンしたコンピュータか、そのコンピュータのアドレスは何か、コンピュータを使用している社員の社員コードは何か、といった情報が含まれる。なお、コンピュータウィルスを発見した場合に、無条件に直ちに感染しているコンピュータを攻撃すると、使用者がとまどって様々な弊害が生じる。そこで、警

報発生手段１９を設ける。警報発生手段１９は、例えば、ポップアップメッセージなどの通知手段を使って、感染コンピュータに対し、「このコンピュータはウィルスに感染しています。早急にネットワークから切り離してください」といった対策開始を予告するメッセージを送信する機能を持つ。さらに、周辺のコンピュータ利用者に対し、ネットワークを通じて、ウィルス７が侵入する恐れがある旨の警告を発するために、例えば、スピーカ２を鳴らしたりディスプレイ３に警報画面を表示したりする機能を持つ。

【００４７】

図２は、検出報告の例を示す説明図である。

通信情報解析手段１６（図１）は、通信情報から取得した送信元ＩＰアドレス８を検出報告送信手段１８に転送する。検出報告送信手段１８は、感染コンピュータ５の管理者に対して、例えば、電子メールやファクシミリを利用して、検出報告を送信する。（ａ）は拡散型のウィルスを検出したときの検出報告例である。（ｂ）は、ネットワーク共有型のウィルスを検出したときの検出報告例である。例えば、（ａ）では、ＩＰアドレスが「192.168.10.15」のコンピュータに、図のようなパタンのウィルスによる攻撃がされている。といった報告である。

【００４８】

[ウィルスの侵入と感染コンピュータの検出]

ウィルスが、ネットワーク上のいずれかのコンピュータに取り込まれると、所定のタイミングで活動を開始する。例えば、ウィルスは、ネットワークを通じて他のコンピュータの共有フォルダをアクセスして、そこに格納されたファイルを書き換えたり破壊したりする。ウィルスが侵入するというのは、このように、共有フォルダをアクセスする行為のことをいう。ウィルスファイルが実際にコピーされるとは限らない。従って、ウィルスが侵入されたコンピュータでは、通常の状態では、ウィルスの侵入によるファイルのアクセスか、正常なファイルのアクセスかを区別できず、ウィルスを検出できないこともある。

【００４９】

そこで、おとりサーバやおとりフォルダを設ける。通常のアプリケーションは、予め特定したサーバやフォルダにのみアクセスする。擬似的に作成された、お

とりサーバやおとりフォルダにアクセスするのは、ウィルスである確率が極めて高い。さらに、そのアクセスパターンを確認することで、ウィルスであるとの確証を得ることができる。その後は、その通信情報から、どのコンピュータがそのウィルスに感染したかを突き止める。感染コンピュータでのウィルスの活動を阻止しなければ、このウィルスがネットワークを通じて様々なコンピュータに被害を及ぼす。

【００５０】

コンピュータ攻撃手段１７（図１）は、感染コンピュータに対して所定の攻撃動作をする機能を持つ。このコンピュータ攻撃手段１７は、感染コンピュータ５に対して、高い負荷をかける。感染コンピュータ中のウィルスの活動を阻止するためであるから、感染コンピュータ５に対して高い通信負荷をかける方法と、感染コンピュータのＣＰＵに高い負荷をかける方法がある。感染コンピュータ５に対して高い通信負荷をかけると、ネットワーク１と感染コンピュータとの間を結ぶネットワークインタフェース１１等の通信路でトラフィックが増大して、感染コンピュータ５からネットワーク１に対する通信の通信速度が著しく低下する。従って、感染コンピュータ内部からネットワーク１を経由して他のコンピュータに向かうウィルスの侵入活動が抑制される。具体的には、１００ＢＡＳＥ－Ｔ程度の帯域を持つネットワークならば、５メガバイト程度もある大きなパケットを感染コンピュータ宛に送信するとよい。しかしながら、この場合、ＣＰＵ自体にはさほどの負荷はかからない。一方、感染コンピュータのＣＰＵに高い負荷をかけると、感染コンピュータの内部でデータの破壊活動をしようとするウィルスの活動速度が著しく低下する。従って、感染コンピュータ中にウィルス被害が広がるのを防止できる。具体的には、２バイト程度のＰｉｎｇパケットを感染コンピュータ５に向けて大量に連続的に送信する。感染コンピュータ５のＣＰＵは、パケットを受信する度に応答を返すための制御をしなければならないので、ＣＰＵが過負荷になる。従って、上記の一方または両方の方法を併用するとよい。もちろん、上記以外の既知の任意の方法で、感染コンピュータに対して、高い負荷をかけるようにしてもよい。

【００５１】

［他のコンピュータによる攻撃］

図３は、複数のコンピュータにより、感染コンピュータ５を攻撃する例を示す説明図である。

図のネットワーク１には、監視コンピュータ１０に感染コンピュータ５のほかに、端末装置２０と端末装置２２と端末装置２４とが接続されている。端末装置２０は、ネットワークインタフェース２１を介してネットワーク１に接続されている。端末装置２２は、ネットワークインタフェース２３を介してネットワーク１に接続されている。端末装置２４は、ネットワークインタフェース２５を介してネットワーク１に接続されている。端末装置２０と端末装置２２と端末装置２４とは、それぞれ、コンピュータ攻撃手段３１とコンピュータ攻撃手段３２とコンピュータ攻撃手段３３とを備えている。コンピュータ攻撃手段３１とコンピュータ攻撃手段３２とコンピュータ攻撃手段３３とはいずれも、監視コンピュータ１０のコンピュータ攻撃手段１７と同様の機能を持つ。

【００５２】

１台のコンピュータで感染コンピュータを攻撃するのが不十分ならば、図のようにして、別のコンピュータに攻撃を依頼して、複数台のコンピュータの協力によって１台のコンピュータを攻撃する。これによって、ウィルスが感染したコンピュータの機能を制限し、その間に管理者に通知して、ウィルスを削除するための時間を稼ぐ。端末装置２０等は、攻撃専用のコンピュータでもよいし、一般ユーザの使用しているコンピュータにコンピュータ攻撃手段３１等をインストールしたものでもよい。監視コンピュータ１０は、ネットワーク１中に１台だけ設けても、複数台設けても構わない。なお、監視コンピュータ１０からコンピュータ攻撃手段３１等に送信する攻撃依頼には、感染コンピュータのＩＰアドレス（ネットワークアドレス）を含める。また、コンピュータ攻撃手段３１等を起動するコマンドを含めるとよい。コンピュータ攻撃手段を持つコンピュータは、監視コンピュータと同様の機能を持つコンピュータでもよいし、攻撃手段のみを持つコンピュータでもよい。

【００５３】

図４は、大規模なコンピュータネットワークの説明図である。

図のように、ルータ５０とルータ５１とにより相互に接続されたネットワーク５２とネットワーク５３とネットワーク５４には、それぞれ、多数のコンピュータが接続されている。ネットワーク５２に接続されたコンピュータ６１と６２のうち、コンピュータ６２は監視コンピュータである。ネットワーク５３に接続されたコンピュータ６３と６４と６５のうち、コンピュータ６３は監視コンピュータである。ネットワーク５４に接続されたコンピュータ６６と６７と６８のうち、コンピュータ６８は監視コンピュータである。例えば、コンピュータ６７が感染コンピュータであって、コンピュータ６２がそのウィルスの侵入を検知することがある。このときは、コンピュータ６２から攻撃をしても、ルータ５０やルータ５１がネックになって、効果的な攻撃が難しい。そこで、コンピュータ６２は、コンピュータ６７の所属するネットワーク５４に接続された最寄りのコンピュータ６８に対して、コンピュータ６７への攻撃を依頼する。コンピュータ６８は先に説明したスピーカ等による警報を発して、周囲のコンピュータ６６等に注意を促してから、コンピュータ６７への攻撃を開始する。こうして、大規模なネットワークにおける監視動作も可能になる。

【００５４】

[動作フローチャート]

図５は監視コンピュータの基本動作を示すフローチャートである。

まず、ステップＳ１において、監視コンピュータ１０は、おとりサーバ１３やおとりフォルダ１４やおとりアプリケーション１５を有効にする初期設定をして、ステップＳ２で、ウィルスの待ち受けを開始する。通信情報解析手段１６は、ネットワークインタフェース１１の処理する通信情報を監視する。ステップＳ３で、ウィルスの侵入を検知すると、通信情報解析手段１６は、ステップＳ４で通信情報の解析をして、ステップＳ５で送信元ＩＰアドレス８を取得し、感染コンピュータを特定する。検出報告送信手段１８は、ステップＳ６で管理者へ検出報告をする。

【００５５】

警報発生手段１９は、ステップＳ７で、スピーカ２による警報音を鳴らす。同時に攻撃中である旨の動画等を、監視コンピュータ１０のディスプレイ３に表示

する。ステップＳ８で、警報発生手段１９は、感染コンピュータ５に対して攻撃開始メッセージを送信する。コンピュータ攻撃手段１７は、ステップＳ９で攻撃を開始する。その後のステップＳ１０で、任意のルートでウィルス対策が完了した旨を報告を受けたと判断すると、ステップＳ１１に進んで、コンピュータ攻撃手段１７による攻撃を終了する。

【００５６】

図６は、監視コンピュータの協力動作を示すフローチャートである。

複数のコンピュータの協力を得て感染コンピュータを攻撃するときは、まず、感染コンピュータを特定する。ステップＳ２１～ステップＳ２４の処理は、ステップＳ２～ステップＳ５の処理と同様である。感染コンピュータを特定したら、ステップＳ２５で、コンピュータ攻撃手段１７がネットワークの調査をする。最寄りの監視コンピュータを探すためである。最寄りの監視コンピュータを探すには、予め用意した監視コンピュータのリストから、感染コンピュータとＩＰアドレスの一部が共通している監視コンピュータを検索する（ステップＳ２６）。

【００５７】

最寄りの監視コンピュータが、自分自身である場合と、図４で説明したように、ルータのような幾つかのネットワークコンポーネントを介して接続された監視コンピュータである場合とがある。ステップＳ２７では、最寄りの監視コンピュータが自分自身かどうかを判断して、自分自身でなかったら、ステップＳ２８で攻撃依頼先を決定する。該当する監視コンピュータが複数ある場合は、複数の監視コンピュータに同報送信で攻撃依頼を発信すればよい。続いて、ステップＳ２９で、該当する監視コンピュータに対して、攻撃依頼の発信をする。その後は、攻撃依頼先において、図５のステップＳ６以降の処理が実行される。

【００５８】

[感染コンピュータの処置]

感染コンピュータは被害を受けている可能性が高いので、すみやかにネットワークから切り離すことが最も効果的な対策である。この対策が完了すれば、感染コンピュータへの攻撃は終了してよい。感染コンピュータは、その後、ウィルスの除去処理をして、被害があった部分を修復したり、ＯＳ（オペレーティングシ

ステム）やアプリケーションの再インストールをして復旧させる。このために、図３に示すように、記憶装置６には、その旨のメッセージを含む画面４０をディスプレイに表示する。この画面４０は、必要な対応措置が終了後ボタン４１がクリックされるまで表示される。

【００５９】

この発明は、ネットワークを通じて拡散するタイプのウィルスの拡散スピードを低下させる機能を持つ。すなわち、ウィルスが感染したコンピュータに大きな負荷をかけることによって、ウィルスの拡散を防止する。また、ウィルスが、あるコンピュータの共有ファイルに侵入しても、その動作だけでは侵入を直ちに確認することができない場合に適する。すなわち、ウィルスが活動したとき、そのウィルスの攻撃を真っ先に受けるようにおとりのコンピュータを設定する。これによって、ウィルスを発見し、ウィルスがどのコンピュータに感染しているかを確認し、該当する攻撃対象のコンピュータを特定する。すなわち、単にフォルダ内に侵入しただけでは、発見の難しいウィルスの検出と排除に有効である。

【００６０】

なお、上記のコンピュータプログラムは、それぞれ独立したプログラムモジュールを組み合わせて構成してもよいし、全体を一体化したプログラムにより構成してもよい。コンピュータプログラムにより制御される処理の全部または一部を同等の機能を備えるハードウエアで構成しても構わない。また、上記のコンピュータプログラムは、既存のアプリケーションプログラムに組み込んで使用してもよい。上記のような本発明を実現するためのコンピュータプログラムは、例えばＣＤ－ＲＯＭのようなコンピュータで読み取り可能な記録媒体に記録して、任意の情報処理装置にインストールして利用することができる。また、ネットワークを通じて任意のコンピュータのメモリ中にダウンロードして利用することもできる。

【図面の簡単な説明】

【図１】　ウィルス対策システムの具体例を示すブロック図である。

【図２】　検出報告の例を示す説明図である。

【図３】　複数のコンピュータにより感染コンピュータを攻撃する例を示す説

明図である。

【図４】　大規模なコンピュータネットワークの説明図である。

【図５】　監視コンピュータの基本動作を示すフローチャートである。

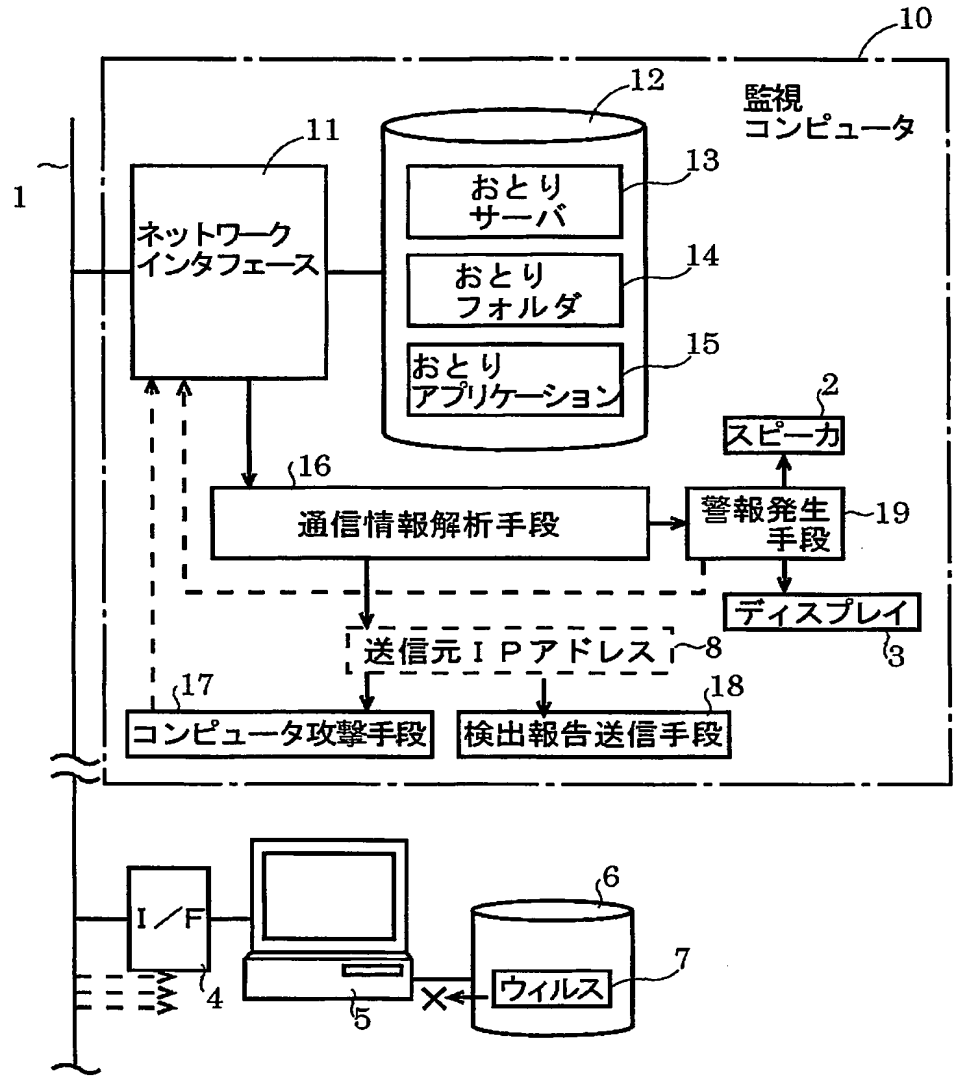
【図６】　監視コンピュータの協力動作を示すフローチャートである。

【符号の説明】

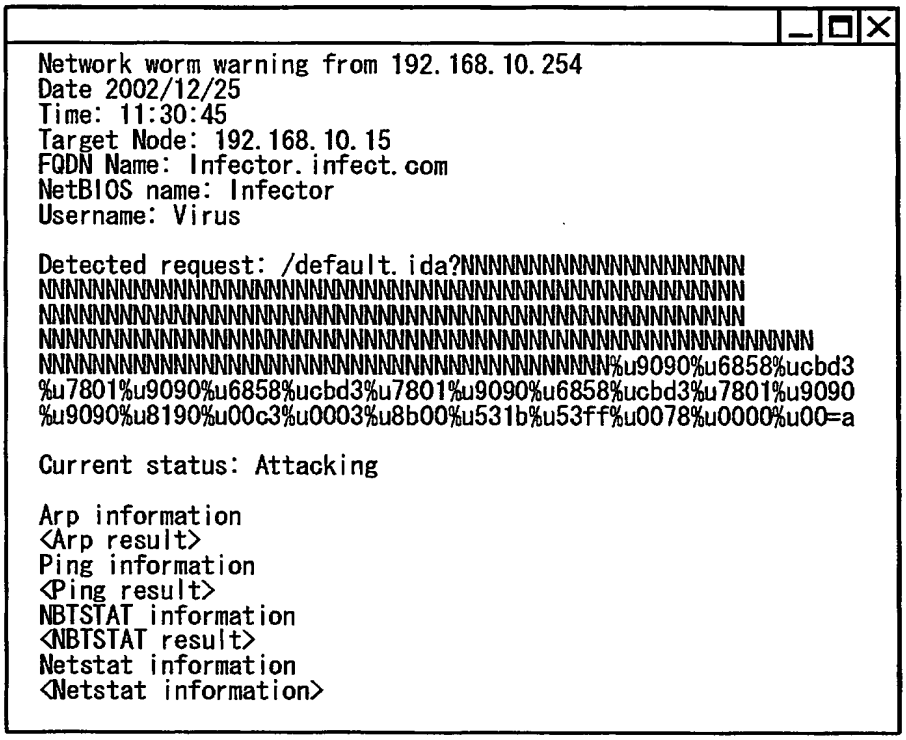
１　ネットワーク、　２　スピーカ、　３　ディスプレイ、　４　ネットワークインタフェース、　５　感染コンピュータ、　６　記憶装置、　７　ウィルス、　８　送信元ＩＰアドレス、　１０　監視コンピュータ、　１１　ネットワークインタフェース、　１２　記憶装置、　１３　おとりサーバ、　１４　おとりフォルダ、　１５　おとりアプリケーション、　１６　通信情報解析手段、　１７　コンピュータ攻撃手段、　１８　検出報告送信手段、　１９　警報発生手段

【書類名】図面

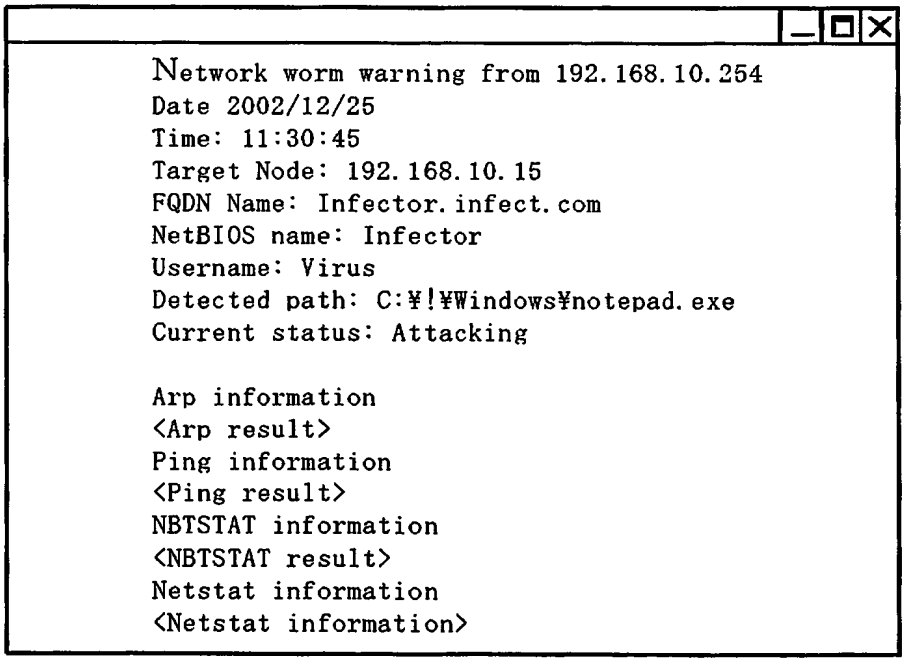
【図１】


10
監視
コンピュータ
12
11
13
おとり
サーバ
1
ネットワーク
インタフェース
14
おとり
フォルダ
15
おとり
アプリケーション
2
スピーカ
16
通信情報解析手段
警報発生
手段
19
ディスプレイ
3
送信元ＩＰアドレス
8
17
18
コンピュータ攻撃手段
検出報告送信手段
I／F
6
4
5
ウィルス
7

【図２】

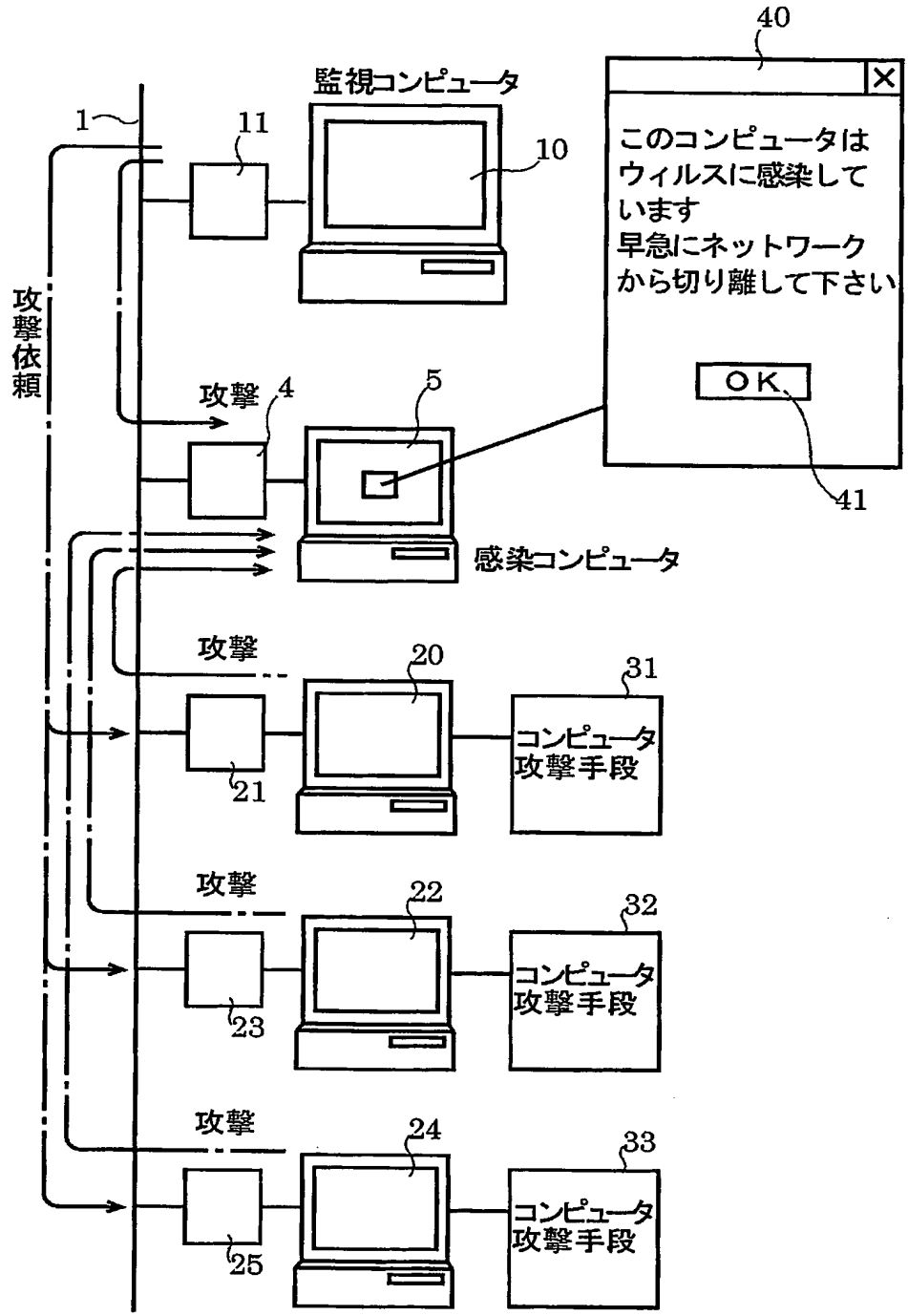

Network worm warning from 192.168.10.254
Date 2002/12/25
Time: 11:30:45
Target Node: 192.168.10.15
FQDN Name: Infector.infect.com
NetBIOS name: Infector
Username: Virus
Detected request: /default.ida?NNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3
%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090
%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
Current status: Attacking
Arp information
<Arp result>
Ping information
<Ping result>
NBTSTAT information
<NBTSTAT result>
Netstat information
<Netstat information>

（ａ）

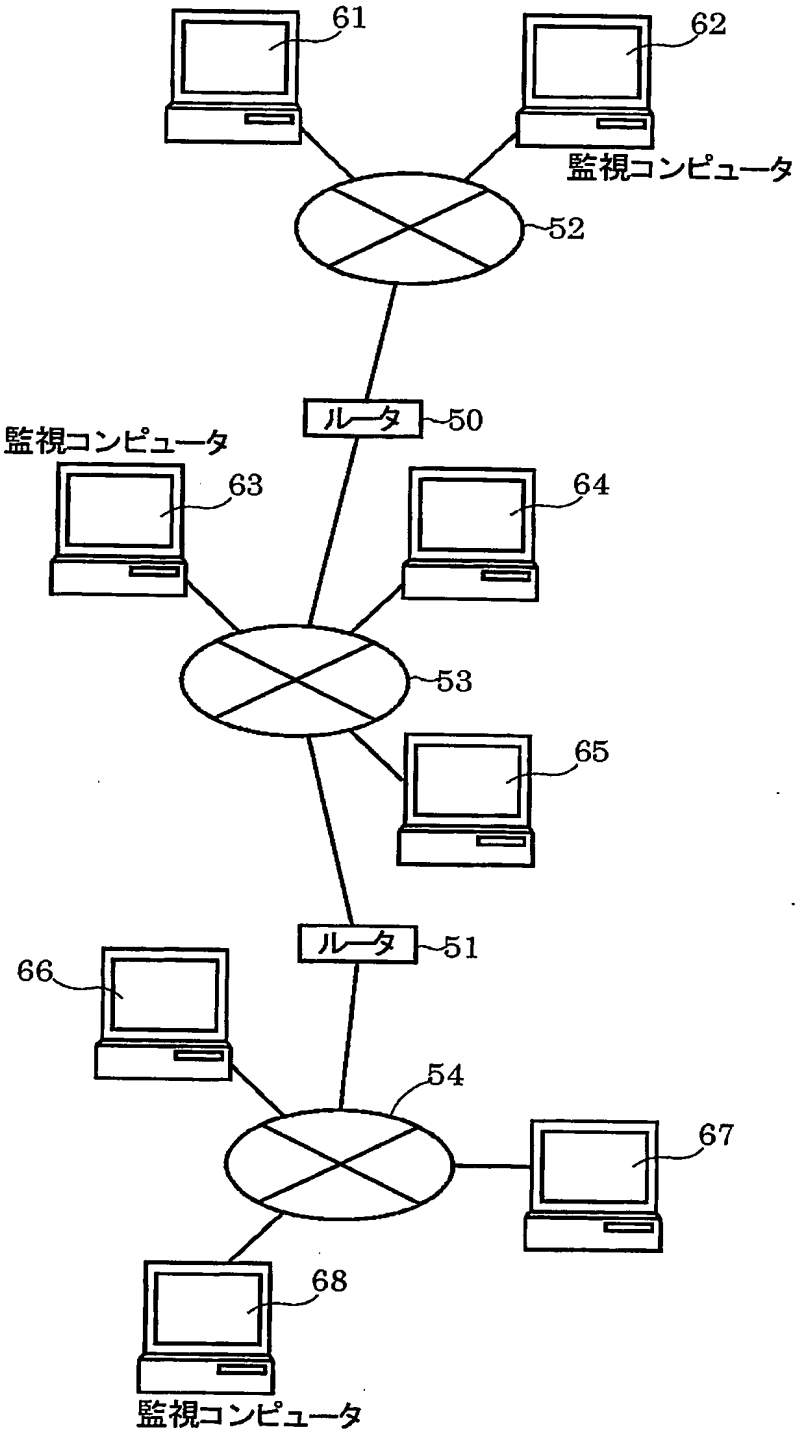

Network worm warning from 192.168.10.254
Date 2002/12/25
Time: 11:30:45
Target Node: 192.168.10.15
FQDN Name: Infector.infect.com
NetBIOS name: Infector
Username: Virus
Detected path: C:¥!¥Windows¥notepad.exe
Current status: Attacking
Arp information
<Arp result>
Ping information
<Ping result>
NBTSTAT information
<NBTSTAT result>
Netstat information
<Netstat information>

（ｂ）

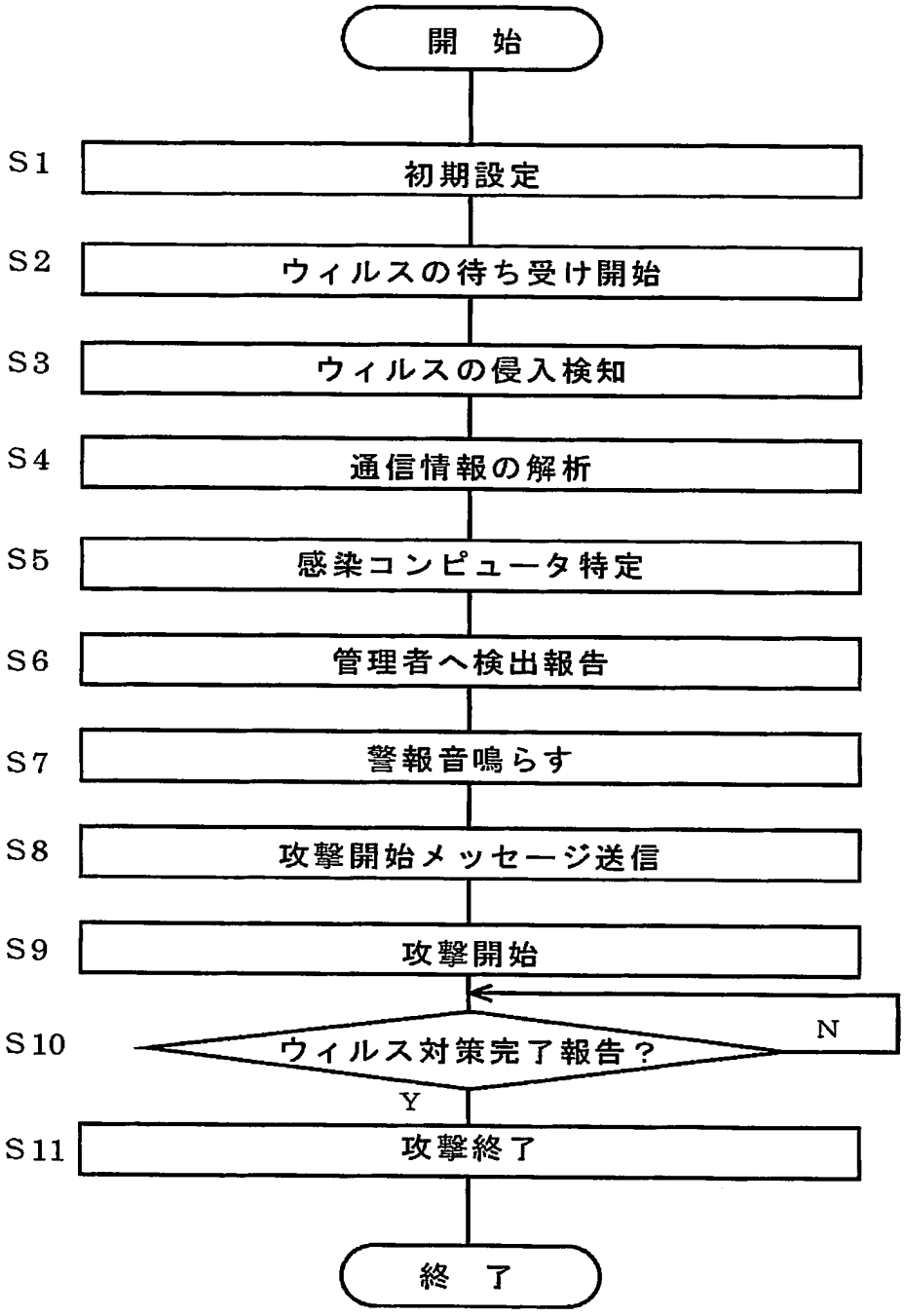
【図３】


40
監視コンピュータ
1
11
10
このコンピュータは
ウィルスに感染して
います
早急にネットワーク
から切り離して下さい
攻撃依頼
攻撃
4
5
OK
41
感染コンピュータ
攻撃
20
31
コンピュータ
攻撃手段
21
攻撃
22
32
コンピュータ
攻撃手段
23
攻撃
24
33
コンピュータ
攻撃手段
25

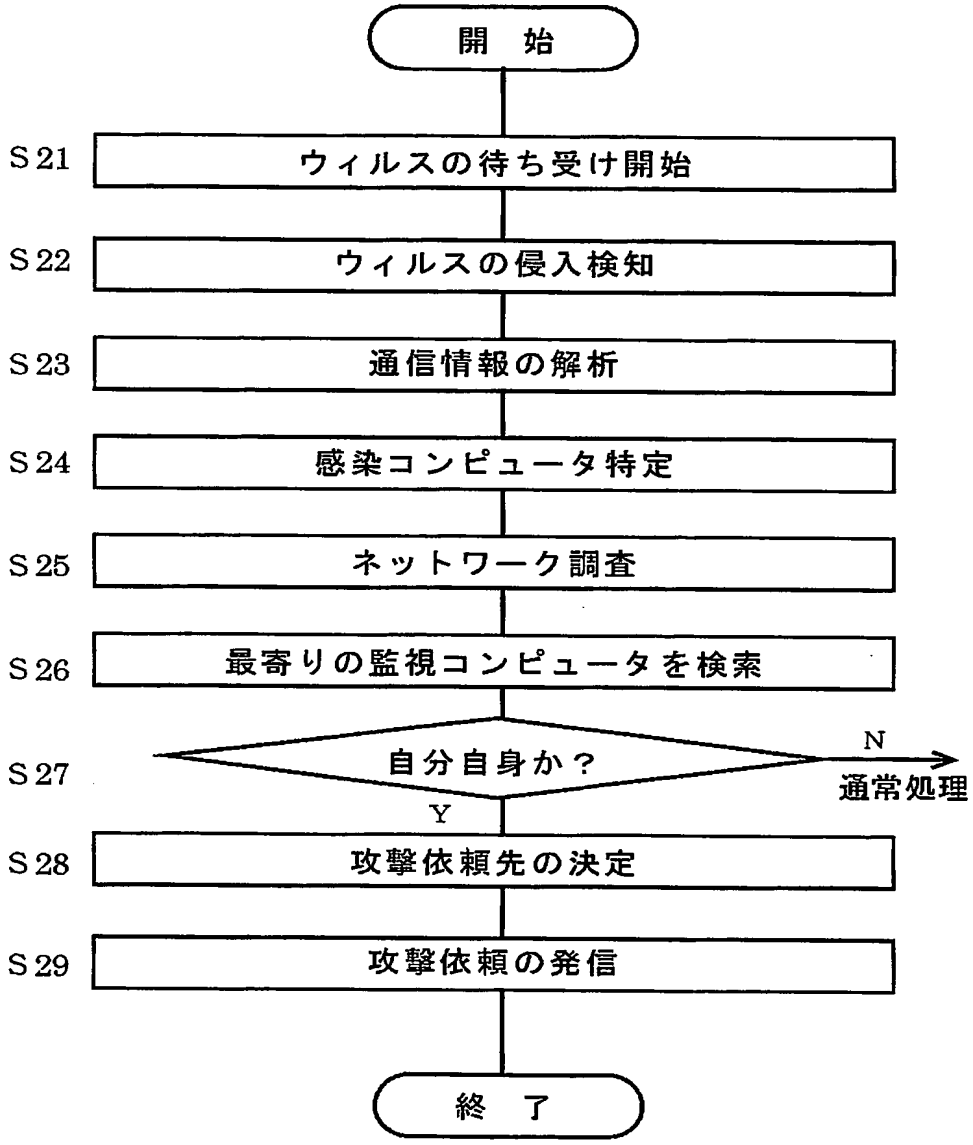
【図４】


61
62
監視コンピュータ
52
ルータ
50
監視コンピュータ
63
64
53
65
ルータ
51
66
54
67
68
監視コンピュータ

【図５】


開　始
S1
初期設定
S2
ウィルスの待ち受け開始
S3
ウィルスの侵入検知
S4
通信情報の解析
S5
感染コンピュータ特定
S6
管理者へ検出報告
S7
警報音鳴らす
S8
攻撃開始メッセージ送信
S9
攻撃開始
S10
ウィルス対策完了報告？
N
Y
S11
攻撃終了
終　了

【図６】


開　始
S21
ウィルスの待ち受け開始
S22
ウィルスの侵入検知
S23
通信情報の解析
S24
感染コンピュータ特定
S25
ネットワーク調査
S26
最寄りの監視コンピュータを検索
S27
自分自身か？
N
通常処理
Y
S28
攻撃依頼先の決定
S29
攻撃依頼の発信
終　了

【書類名】　要約書

【要約】

【課題】　ネットワーク１を通じてサーバやフォルダに侵入するウィルスをいちはやく検出して、被害の拡大を抑える。

【解決手段】　ウィルスに感染しているコンピュータ５を特定し、そのコンピュータ５の管理者がウィルスを除去する等の対策を終了するまでの間、監視コンピュータ１０による攻撃を行う。そのコンピュータ５に高負荷を生じさせて、ウィルス７の活動を抑制する。ウィルス７に感染しているコンピュータ５を特定するためには、おとりのサーバ１３等をネットワーク１中に構築する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０７２３７１
受付番号	５０３００４３３９３６
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　３月１８日

＜認定情報・付加情報＞

【提出日】　平成15年 3月17日

次頁無

特願２００３－０７２３７１

出　願　人　履　歴　情　報

識別番号　［０００００２３６９］

１．変更年月日　１９９０年　８月２０日
［変更理由］　新規登録
住　所　東京都新宿区西新宿２丁目４番１号
氏　名　セイコーエプソン株式会社